

Certification and Accreditation of PIV Card Issuing Organizations

Joan Hash

Manager, Computer Security Management
& Assistance

June 28, 2005

NIST Special Publication 800-79

On June 17, 2005, NIST posted the Draft

“Guidelines for the

*Certification and Accreditation of PIV
Card Issuing Organizations”*

on WWW.CSRC.NIST.GOV/PIV-Project

for comment before July 10, 2005

What is a PIV Card Issuer?

- A Federal organization or contractor authorized to issue identity cards:
 - in accordance with the policy established in Homeland Security Presidential Directive 12 ;
 - using identity authentication and verification procedures that comply with the requirements of Federal Information Processing Standard 201;
 - utilizing technical specifications that conform with FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78.

Why PIV Card Issuer Accreditation?

- Homeland Security Presidential Directive 12 requires PIV Cards to be issued only by providers whose reliability has been accredited.
- Accreditation will help to assure competence, confidence in, and equivalence of PIV Card Issuer
- Accreditation will provide additional trust of one agency for the PIV Cards issued by other agencies

What is PIV Issuer Accreditation?

PIV Issuer Accreditation is the official management decision of the Designated Accreditation Authority to authorize operation of a PIV Card Issuer after determining that the Issuer's reliability has satisfactorily been established through appropriate assessment and certification processes.

What is PIV Issuer Certification?

Certification of a PIV Issuer is a formal process of assessing the attributes (e.g. knowledge, capability, availability, personnel, equipment, finances, and adequately supported infrastructures) of a PIV Card Issuer using various methods of assessment (e.g., interviews, document reviews, laboratory test results, procedure evaluations, component validation reports) that support the assertion that the PIV Card issuing organization is reliable and capable of enrolling approved applicants and issuing secure PIV Cards in accordance with FIPS 201.

When Should Accreditation be Done?

- Accreditation is required before a PIV Card Issuer may issue operational PIV Cards.
- Accreditation should be repeated within a time period established by the Designated Accreditation Authority of the agency using the services of a PIV Card Issuer.
- Accreditation must be repeated when a major change is made to the PIV Card Issuer's operations or major problems are identified.

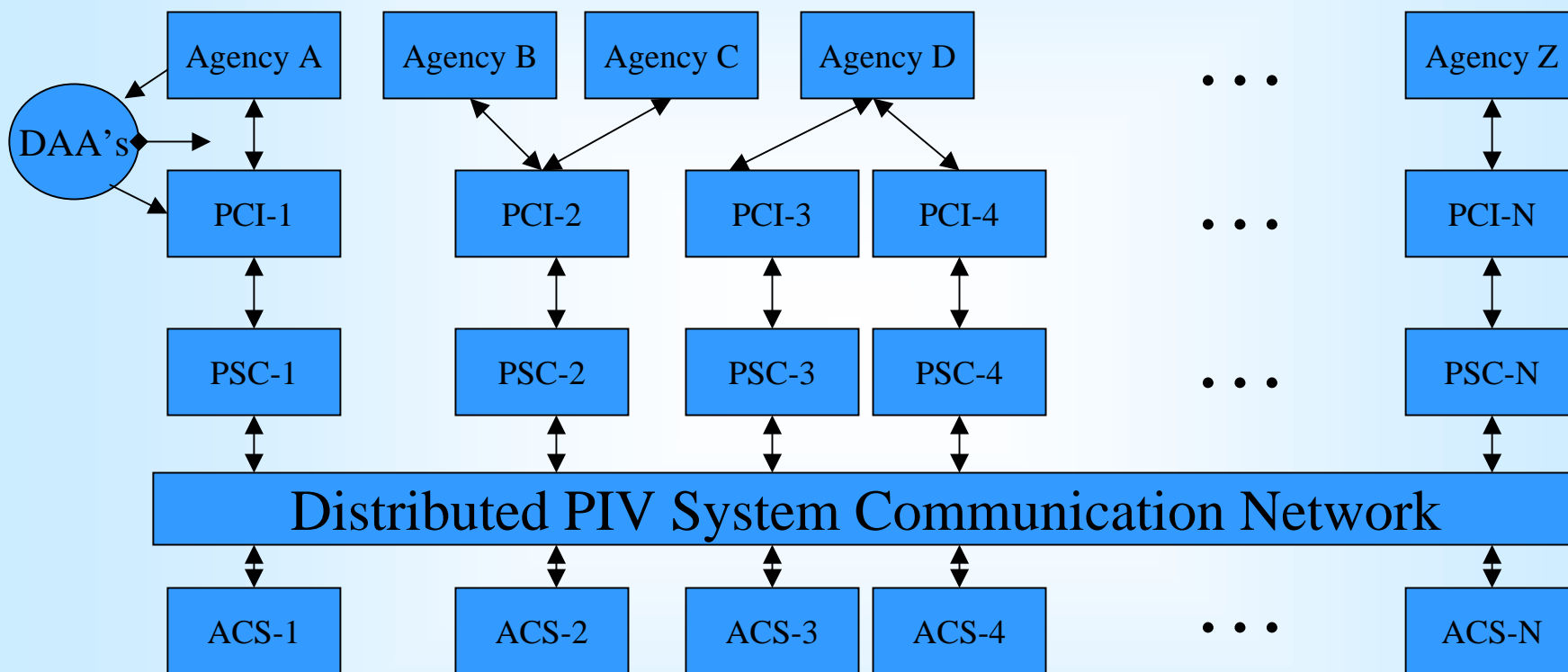
What is the PIV System?

The PIV System may be viewed logically as a single, integrated, interoperable automated system with common objectives, policies, communication protocols, and application programs

WITH

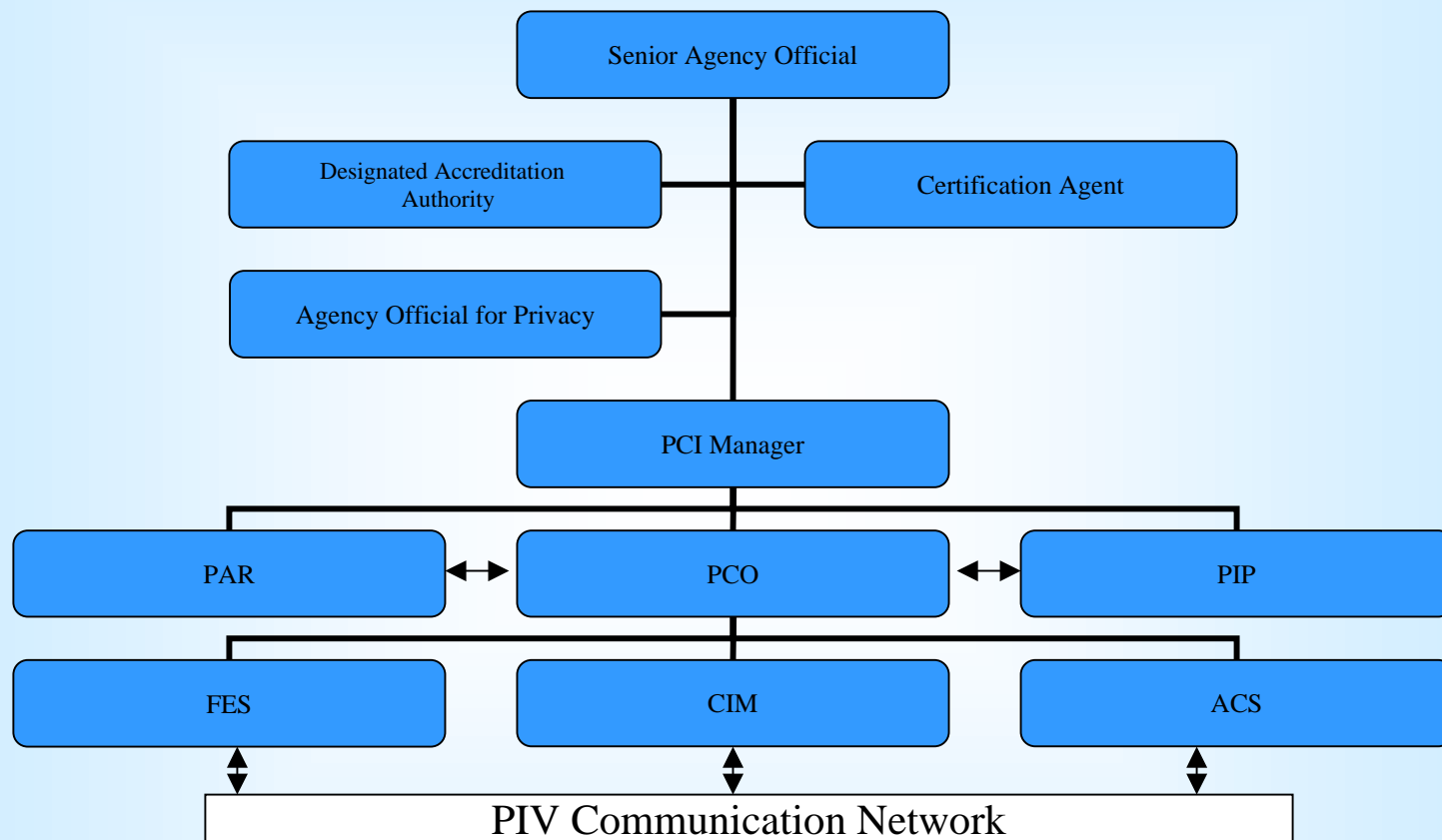
independently managed computer systems containing independently manufactured components that will change as new technology becomes available and agencies desire additional services.

A Logical View of the PIV System



DAA: Designated Accred. Auth.; PCI: PIV Card Issuer; PSC: PCI Computer Support; ACS: Access Control Systems

Sample PIV Card Issuing Organization and Roles



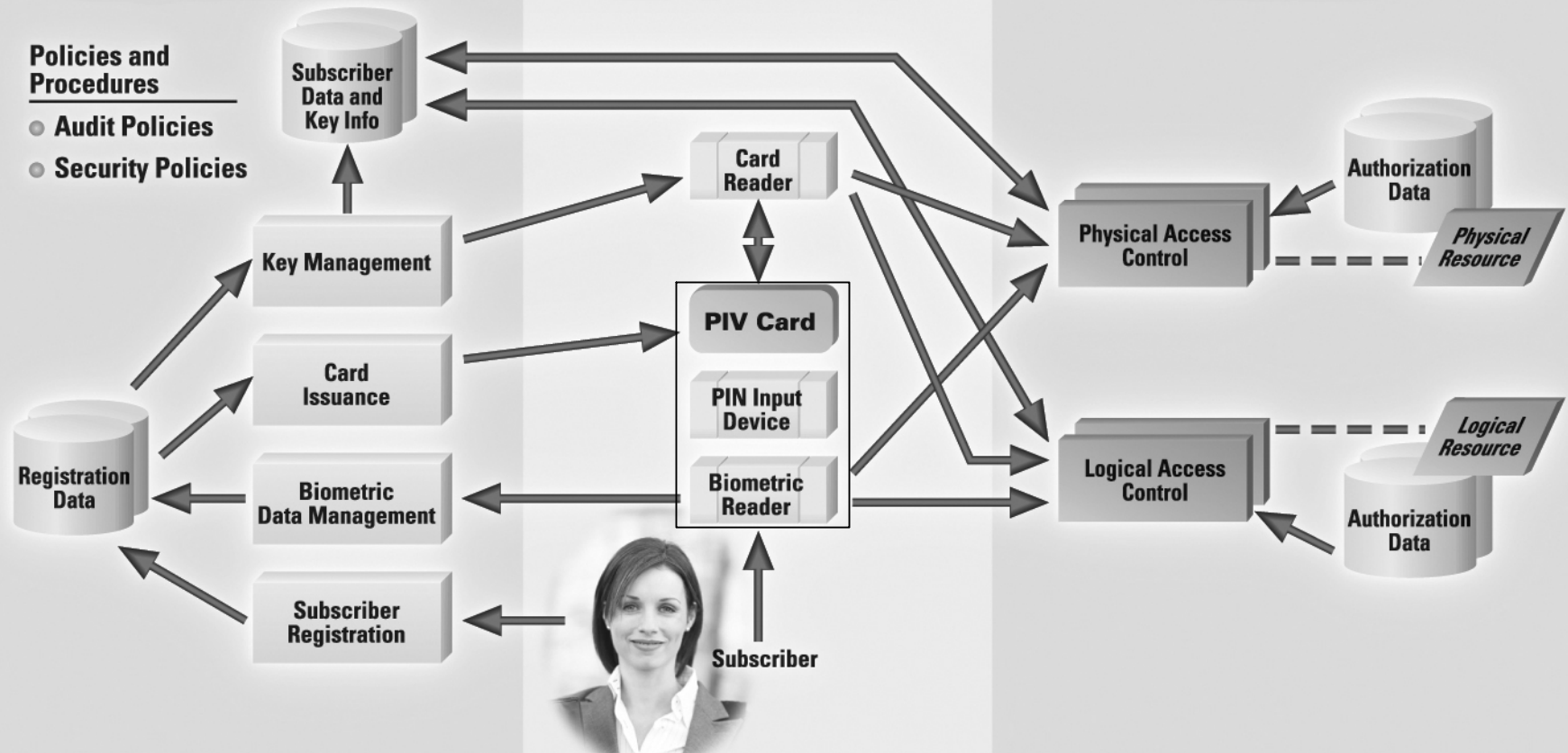
PAR: PIV Applicant Registrar; PCO: PIV Card Operations; PIP: PIV Identity Proofing; FES: PIV Front End System; CIM: Card Issuance & Management; ACS: Access Control System

PIV System Concept and Model

PIV Card Issuance and Management Infrastructure

Subscriber and PIV Card

PIV Card Operation/Use Infrastructure



Vocabulary

- Assessment

- determination of an organization's capability, competence, reliability, compliance with standard procedures, and use of products conforming with specifications of a standard.

- Validation

- determination of a product's or a service's conformance to standards

Vocabulary

- Compliance
 - Status of an organization when it has implemented and is using a standard in a manner that satisfies its requirements.
- Conformance
 - Status of a product or a service when it has been designed, implemented, and is being used in a manner that satisfies the specifications of a standard.

Required/Desired Attributes of a PIV Issuer

- Reliability of a PIV Issuer is exhibited by its being
 - Knowledgeable (R)
 - Capable (R)
 - Available (R)
 - Legal (R)
 - Compliant (R)
 - Adequately Supported (R)
 - Prepared/responsive/efficient (D)
 - Adaptable (D)
 - Cost Effective (D)

Methods of Assessing Attributes

- Review and Analysis
- Interview
- Demonstration/Direct Observation
- Sampling/Statistics
- Testing/Validation
- Evaluation/Measurement
- Compliance/Conformance with standards
- Precedence/Accepted Practice
- Experience

Phases of Certification and Accreditation

- Initiation Phase

- Identify Resources (Create C & A Team)
 - Designated Accreditation Authority
 - Certification Agent
 - PIV Card Issuer Manager
 - PIV Card Applicants Representative
- Collect Relevant Standards, Guidelines, etc.
- Obtain PIV Card Issuer's Operational Plan
- Create Certification Plan

Phases of Certification and Accreditation

- Certification Phase
 - Select the Attributes of the PIV Issuer to be Assessed
 - Select the Assessment Methods to be Used
 - Apply selected assessment methods to:
 - PIV Card Issuer Personnel, Documentation,
 - Planned Services, Operational Plan
 - Prepare Assessment Reports
 - Provide to PIV Card Manager

Phases of Certification and Accreditation

- Accreditation Phase

- Review the results of the certification phase
- Review the residual risks expected after reducing discovered vulnerabilities
- Review the accreditation documentation
- Make an accreditation decision
- Authorize to Operate if risks are acceptable
- Interim Authorization to Operate if correctable
- Deny Authorization to Operate if unacceptable

Phases of Certification and Accreditation

- Monitoring Phase

- Perform PIV Card issuing services in compliance with FIPS 201
- Monitor security and operating procedures
- Sample and evaluate PIV Card production
- Report results to PIV Card Issuer Manager
- PIV Card Issuer Manager should report significant problems to Designated Accreditation Authority

Authorization to Operate Alternatives

- The agency's Designated Accreditation Authority issues to a PIV Card Issuer:
 - An Authorization to Operate if fully accredited after its reliability has been certified;
 - An Interim Authorization to Operate under specific terms and conditions (not accredited);
 - A Denial of Authorization to Operate if the assessments are unsatisfactory.

Certification & Accreditation Tasks

- Preparation
- Resource Identification
- PCI Operations Plan Review
- PCI Attribute Assessment
- Certification Documentation
- Accreditation Decision
- Accreditation Documentation
- PCI C & A Management and Control
- PCI Attribute Monitoring
- Status Reporting

Certification & Accreditation

- Should be a part of normal organizational and computer system management.
- Should be conducted as a normal part of organization assessment and evaluation.
- Should be performed initially to verify that FIPS 201 is being implemented and used properly.
- Should be performed periodically to verify that all PCI's are complying with FIPS 201 equivalently.
- Should help assure an agency that PIV Cards issued by other agencies may be Trusted.

Summary of Certification & Accreditation

- The Reliability of PIV Card Issuing Organizations must be accredited in accordance with NIST SP 800-79 before they can perform FIPS 201 Services.
- The Security of the PIV Card Issuing Organization's Computer Systems must be accredited consistent with NIST SP 800-37.

Solicitation for Comments on SP 800-79

- NIST posted Special Publication 800-79 entitled ***“Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations”*** on its Website

www.csrc.nist.gov/PIV-Project

for comment on June 17, 2005

- ***Comments are due in electronic form by July 10, 2005***

How to Submit Comments

See: WWW.CSRC.NIST.GOV/PIV-Project

Read: Questions and Answers on PCI C & A

Read: Draft NIST SP 800-79

Load: Excel PIV Comment Form from Website

Input: Name, Org., Comments etc. into Form

Save: Save Completed Form on Computer

Send: Comment Form in e-mail attachment to
PIVaccreditation@Nist.Gov